

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

Present: The Honorable Lisa Bredahl	ANDREW J. GUILFORD Not Present	
Deputy Clerk	Court Reporter / Recorder	Tape No.
Attorneys Present for Plaintiffs:	Attorneys Present for Defendants:	

Proceedings: [IN CHAMBERS] CLAIM CONSTRUCTION ORDER

mSIGNIA alleges that InAuth has infringed Claims 1–6, 13–15, and 17–25 of U.S. Patent No. 9,559,852 (“the ’852 Patent”). (Dkt. 1.) InAuth counterclaimed for declaratory judgment of non-infringement and invalidity of the ’852 Patent. (Dkt. 23.) Before the Court is the issue of claim construction. This Order addresses the terms at issue.

1. LEGAL STANDARD

Claim construction is the process of determining the meaning and scope of patent claims. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 976 (Fed. Cir. 1995) (en banc), *aff’d*, 517 U.S. 370 (1996). It is a matter for the court. *Id.* at 979.

The words of a claim are given their ordinary and customary meaning as understood by a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005). In some cases, this may “be readily apparent even to lay judges, and claim construction in such cases involves little more than the application of widely accepted meaning of commonly understood words.” *Id.* at 1314. But it “often requires the judge only to examine and to construe the document’s words” *Teva Pharms. USA, Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 840–41 (2015).

Although claims are read in light of the specification, limitations from the specification must not be imported into the claims. *Comark Commc’ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1186–87 (Fed. Cir. 1998). For the specification to define a term to mean something other than its ordinary meaning, it must set out its definition in a manner sufficient to provide notice of that

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

meaning to a person of ordinary skill in the art. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

The prosecution history is also a part of the intrinsic evidence consulted during claim construction. *See Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1324 (Fed. Cir. 2002). But “because the prosecution history represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, it often lacks the clarity of the specification and thus is less useful for claim construction purposes.” *Phillips*, 415 F.3d at 1317. “[W]hen the patentee unequivocally and unambiguously disavows a certain meaning to obtain a patent, the doctrine of prosecution history disclaimer narrows the meaning of the claim consistent with the scope of the claim surrendered.” *Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1359 (Fed. Cir. 2017) (quoting *Biogen Idec, Inc. v. GlaxoSmithKline LLC*, 713 F.3d 1090, 1095 (Fed. Cir. 2013)) (finding prosecution history disclaimer may be based on a patent owner’s statements during *Inter Partes* Review proceedings).

2. BACKGROUND

The ’852 Patent issued January 31, 2017 and is titled “Cryptographic Security Functions Based on Anticipated Changes in Dynamic Minutiae.” The ’852 Patent describes using “dynamic key cryptography” to, for example, authenticate a client’s (“service user’s”) electronic device so that it is recognized by a service provider. *See, e.g.*, ’852 Patent at 1:20–25. In some examples, the ’852 Patent refers to using computer “minutia” to recognize and authenticate a particular user or computer. *Id.* at 5:64–67. The patent describes “computer and user minutia” as “any piece of information that can be definitively associated with the computer and its user, including information from the general categories of what the user or computing device has, what the user knows, and what the user is.” *Id.* at 6:31–35. The patent explains that rather than using a static username and password combination, or some other “static key” stored on the computer, detecting a very large range of minutia values can provide better security against counterfeits. It also means a user doesn’t have to worry about remembering a password. *Id.* at 5:66–6:3, 5:29–35. A computer’s minutiae, however, “can (and are expected to) change and evolve over time.” *Id.* at 6:40–42. If the minutiae are evaluated at a single point in time as a “static” collection of values, but some measured

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

minutiae change, this can result in a computer being falsely identified as different when it is actually the same computer. *Id.* at 2:60–65. To address this issue, the ’852 Patent describes embodiments that anticipate changes to minutiae. *See, e.g., id.* at 6:44–48.

The ’852 Patent includes three independent claims (Claims 1, 24, and 25). The remaining claims (Claims 2–23) are dependent claims that depend either directly or indirectly from Claim 1. Claim 1 is illustrative and recites:

1. An identity recognition system comprising:
 - a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes (a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity;
 - one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of identity information by a computer is authentic, by performing operations comprising:
 - generating a challenge to the computer, wherein the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the stored data values associated with the identity;
 - receiving, from the computer, the response to the challenge;
 - determining whether the response is allowable, wherein such determining comprises using the stored information regarding anticipated changes to the stored data values associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value;
 - and

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

recognizing that the presentation of identity information by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.

'852 Patent, Claim 1.

3. ANALYSIS

3.1. Agreed Constructions

The parties agree to the construction of one term:

Claim Term	Parties' Agreed Construction
“generating a challenge” (Claims 1, 24, and 25)	“generating a request for information”

The Court sees no facial issues with the parties' agreed proposed construction.

3.2. Disputed Terms

3.2.1. “information regarding anticipated changes to one or more of the stored data values associated with that identity” (Claims 1, 24, and 25)

mSIGNIA's Proposed Construction	InAuth's Proposed Construction
No construction necessary	“predictions of what one or more stored values associated with that identity may change to in the future, and when, not including backwards-looking information about changes after they occur used to determine whether a threshold has been met”

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

InAuth focuses the entirety of its briefing for the term “information regarding anticipated changes to one or more of the stored data values associated with that identity” on a prosecution disclaimer argument. (*See* Dkt. 37 at 11–15; Dkt. 39 at 1–8.) InAuth argues that mSIGNIA’s statements distinguishing prior art in an IPR proceeding created a clear and unequivocal disavowal of claim scope, necessitating InAuth’s narrower proposed construction. (*Id.*)

In skipping ahead to this prosecution disclaimer argument, InAuth doesn’t dispute that the patent claims and specification support mSIGNIA’s position. Claim 1 itself spells out that the claimed system relates to storing information regarding anticipated changes to “stored data values” and determining whether a computer’s “response” to a “challenge” is an “allowable response” based on whether the computer’s stored data values are “based on [] acceptable change[s].” ’852 Patent, Claim 1. Many of the dependent claims also shed light on the meaning of the disputed “information regarding anticipated changes . . .” phrase. Some of the dependent claims, for instance, discuss what types of data values might constitute acceptable changes to data values. *See, e.g., id.* at Claims 8–12. Other dependent claims discuss the timing for computing what would constitute an “allowable response.” *See id.* at Claims 15–16. Other dependent claims refer to using information from an allowable response to update the system’s stored information regarding anticipated changes. *See id.* at Claims 22–23. The claim language itself appears to use the claim phrase in its ordinary sense, and InAuth has not argued otherwise.

The specification doesn’t support all of InAuth’s proposed limits to the claim phrase. For instance, one passage states, “[t]he dynamic key cryptography system according to one embodiment ***anticipates changes*** to the minutia caused by updates ***and natural usage*** of the computer.” ’852 Patent at 5:17–18 (emphasis added). The ’852 Patent also refers to an embodiment that

[g]ather[s] industry information regarding updates to computer hardware, firmware and software to create a catalogue of industry minutia values which may possibly appear on registered computers when they are updated. ***The***

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

catalogued industry minutia values are indexed and the possible minutia and current minutia are combined and permutations intelligently stored to anticipate future minutia possibilities.

Id. at 8:8–15 (emphasis added); *see also id.* at 9:6–9 (“One embodiment uses a computer identity provider service to collect computer minutia information from the industry and uses this data to anticipate possible changes and permutations to minutiae on registered computers.”). The ’852 Patent elsewhere describes an embodiment that “models predictive and anticipated changes that occur naturally and during the use of a computer or device.” *Id.* at 8:66–9:1. (Of note in this passage, the specification uses both the terms “predictive” and “anticipated,” perhaps to mean different things.) In another passage describing a particular embodiment, the ’852 Patent also states,

selection of minutia may use *expectations for changes to the current minutia [] 70 database based on knowledge of the current computer minutia 64, current secrets and biometric minutia 26 and knowledge of all minutia value updates that can occur (i.e. anticipated minutia [database])*. Knowledge of all minutia value updates that can occur, *whether or not the updates actually have occurred*, can be gained from the previously mentioned collecting and cataloging industry-wide of all computer minutia updates and the heuristically determined trends caused by the use of computer **18** by a particular service user **20**.

Id. at 14:14:51–64 (emphasis added). These citations would all suggest that InAuth’s proposed construction is unnecessarily limiting.

But as mentioned, InAuth doesn’t address any of these citations. Instead, InAuth goes straight to statements made by mSIGNIA in a Patent Owner Preliminary Response (“POPR”) in an IPR proceeding. InAuth argues that there were three disclaimers in claim scope in the POPR: 1) mSIGNIA equated “information regarding anticipated changes” to “predictions” of changes that may occur in the future; 2) mSIGNIA made statements limiting the term to require a prediction as to “what” data may change and “when”; and 3) mSIGNIA disclaimed

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

“backwards-looking information about changes after they occur, used to determine whether a threshold has been met.” (*See* Dkt. 37 at 11–15; Dkt. 39 at 5–8.)

In the POPR, mSIGNIA explained that prior art systems “either had fingerprints that were too short-lived due to changing data, or had fingerprints that would accept *any* value because the system could not anticipate (i.e., expect, predict) how the data value would change.” (Dkt. 36-2 (POPR) at 2 (emphasis in original).) In distinguishing a prior art reference to Etchegoyen, mSIGNIA further stated, “Etchegoyen’s methodology does not rely on information regarding anticipated (i.e., predicted, foreseen, expected) changes to a specific data value; instead, Etchegoyen gives rules on what changes are *acceptable* to the group as a whole, but without actually *anticipating* any changes for any of the stored data values.” (*Id.* at 8–9 (emphasis in original).) Elsewhere, mSIGNIA also distinguished Etchegoyen by stating,

[f]or example, Etchegoyen does not provide or rely on any prediction of *how* a given data value will change; *whether* a given data value will change; *what* the data value is expected to change to (e.g., the new serial number of a new graphics card); *why* the expected data value is expected to change, *when* the change is likely to occur, or how time will impact a data value. Indeed, the categorization does not provide or rely on information about the actual probability or even the general likelihood of a change occurring.

(*Id.* at 8 (emphasis in original).)

InAuth’s first argument (equating “anticipate” and “predict”), which relates to some of these excerpts, is unpersuasive. InAuth does not provide a sufficient basis for swapping out the phrase “information regarding anticipated changes,” as used in the claims, for the word “predictions.” Indeed, portions of the POPR that InAuth cites for its argument also refer to “foreseen” and “expected.” InAuth does not explain how the POPR expressly defined “anticipate” to mean “predict” but not these other words. Ultimately, the Court is not sure what difference the parties actually see in the meanings of the two words (indeed, mSIGNIA refers to “predict” and “anticipate” as “synonyms” (Dkt. 38 at 2)), but to the extent the parties perceive a difference in the overall claim phrase and the term “predictions,” InAuth has not

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

shown a clear and unequivocal disclaimer in the POPR that would demand departing from the claim language itself.

Regarding InAuth’s proposed limitations requiring that “information regarding anticipated changes” must include *what* the stored values will change into and *when* the stored values will change, InAuth’s arguments are similarly unpersuasive. For its “what” argument, InAuth extrapolates from statements in the POPR where mSIGNIA distinguished the prior art on the basis that the prior art systems don’t anticipate changes to minutiae. InAuth also points to mSIGNIA’s use of the word “what” in a POPR assertion that “‘permitting any change’ or ‘tolerat[ing] a wide range of changes’ is ‘not using anticipated changes to determine ***what is acceptable.***’” (Dkt. 39 at 7 (citing Dkt. 36-2 at 28–29).) For its “when” argument, InAuth hones in on a single sentence in the POPR where mSIGNIA explained that another prior art reference “does not describe anticipated changes to location; it merely provides a timing threshold, but does not anticipate when the change will occur.” (*Id.* at 23.) These arguments rely on a thin reading of the record and a painfully literal review of places in the POPR where mSIGNIA used the words “what” and “when.” mSIGNIA’s statements distinguished the phrase “anticipated changes” from prior art that relied on monitoring whether a system met a threshold, either as to timing values or collective data values. Indeed, as mSIGNIA notes, its POPR otherwise refers to a series of “criteria for how information about anticipated changes could be satisfied,” including “whether, what, why, when, ***or*** how.” (Dkt. 38 at 2–3; *see also* Dkt. 36-2 at 8.) InAuth has failed to submit sufficient evidence or explanation to show that mSIGNIA’s other POPR statements should be considered a clear or unequivocal disavowal of claim scope regarding the phrase “information regarding anticipated changes.”

To support InAuth’s third argument, InAuth relies on another portion of the POPR where mSIGNIA stated, “Etchegoyen’s system was completely incapable of anticipating a change to any of the data values at issue. Etchegoyen’s analysis only uses backwards-looking information about the changes *after they occur* to determine whether a threshold has been met.” (*Id.* (emphasis in original).) The Court is slightly perplexed by InAuth’s insistence on including this limitation in the construction of this term. The plain meaning of the phrase “information regarding anticipated changes” would suggest that the database relates to anticipating what minutiae might do in the future as opposed to evaluating changes after they occur. In other

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

words (and mSIGNIA seems to agree), mSIGNIA’s statements were not a disclaimer because, on its face, this claim limitation is already directed to something different than using backwards-looking information about changes after they occur to make an evaluation. Prosecution history disclaimer relates to “precluding patentees from recapturing through claim interpretation specific meanings disclaimed during prosecution.” *Omega Eng’g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1323 (Fed. Cir. 2003). Whether claim language on its face is already tailored or different so that it couldn’t cover a particular meaning in the first place presents a different, threshold question. That’s the situation here, and in these circumstances, prosecution history disclaimer doesn’t even come into play.

InAuth asserts that this dispute is relevant because “InAuth’s accused products – like the *Etchegoyen* prior art – only use information gathered *after* the changes have been recognized, rather than predicting changes *before* they occur.” (Dkt. 39 at 3.) At the hearing, InAuth pointed to some deposition testimony citations in its opening brief to support this assertion. (See Dkt. 37 at 8–9 (citing Dkt. 37-10).) Even if the Court were to consider InAuth’s cited testimony, there’s still not sufficient information for the Court to adequately evaluate either InAuth’s assertions or its witnesses’ statements at this stage. Although this may ultimately be the case and lead to “mischief” on mSIGNIA’s part, the time isn’t ripe to consider it. The Court will not rely on this argument or evidence regarding the functioning of the accused product to influence its claim construction analysis.

Ultimately, InAuth’s arguments either don’t relate to disclaimers or relate to concerns that appear to be inconsistent with even a plain and ordinary understanding of the claim phrase. Moreover, InAuth’s proposed construction doesn’t quite roll off the tongue. In addition to the other issues with InAuth’s proposed construction, the Court has concerns that a juror reading “predictions of what one or more stored values associated with that identity may change to in the future, and when, not including backwards-looking information about changes after they occur[,] used to determine whether a threshold has been met” would simply be confused about the proper scope of the term or feel that this construction implies a more limited scope than InAuth even intends.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

At the hearing, InAuth urged the Court to at least adopt a claim construction that included the phrase “not including backwards-looking information about changes after they occur used to determine whether a threshold has been met.” After further considering the issue, the Court continues to agree with mSIGNIA that the term would be better understood by a jury by reference to the term itself in the context of the surrounding claim language.

After considering the parties’ arguments, the Court concludes that no construction is necessary for the term “information regarding anticipated changes to one or more of the stored data values associated with that identity.”

3.2.2. “wherein such determining comprises using the stored information regarding anticipated changes to the stored data values . . .” (Claims 1, 24, and 25)

In their briefs, the parties address the three “wherein such determining . . .” terms together. The Court will do the same.

- **“wherein such determining comprises using the stored information regarding anticipated changes to the stored data values associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value” (Claim 1)**

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

mSIGNIA's Proposed Construction	InAuth's Proposed Construction
No construction necessary.	“wherein such determining comprises using the stored predictions associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value, but not including a determination made by looking for and rejecting unacceptable changes”

- **“wherein such determining comprises using the stored information regarding anticipated changes to the stored data values to determine whether a data value used to form the identity claim is based on an acceptable change to a corresponding stored data value associated with the identity” (Claim 24)**

mSIGNIA's Proposed Construction	InAuth's Proposed Construction
No construction necessary	“wherein such determining comprises using the stored predictions associated with the identity to determine whether a data value used to form the identity claim is based on an acceptable change to a corresponding stored data value associated with the identity, but not including a determination made by looking for and rejecting unacceptable changes”

- **“wherein such determining comprises using the stored information regarding anticipated changes to the stored data values to determine whether a data value upon which the communication is based reflects an acceptable change to a corresponding stored data value associated with the identity” (Claim 25)**

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

mSIGNIA's Proposed Construction	InAuth's Proposed Construction
No construction necessary	“wherein such determining comprises using the stored predictions associated with the identity to determine whether a data value upon which the communication is based reflects an acceptable change to a corresponding stored data value associated with the identity, but not including a determination made by looking for and rejecting unacceptable changes”

The parties’ dispute regarding the three “wherein such determining . . .” terms is very similar to their dispute regarding the “information regarding anticipated changes . . .” term. Namely, InAuth argues that mSIGNIA made a clear and unequivocal disclaimer of claim scope in its POPR during IPR proceedings.

The claim language itself sums up the meaning of these claim phrases. InAuth has not cited any portions of the specification limiting the meaning of the terms as it proposes, and the Court doesn’t find any, either. Because the Court has already explored the specification’s disclosure regarding the similar term “information regarding anticipated changes . . .,” it will turn directly to InAuth’s prosecution disclaimer argument.

InAuth’s argument relies on two sentences in the introduction of mSIGNIA’s POPR distinguishing a prior art reference by stating that the prior art system “(1) does not anticipate any changes; and (2) does not even look for acceptable changes. Instead, it merely rejects unacceptable changes, just like a username/password system or any other prior art authentication system.” (Dkt. 36-2 at 3.) InAuth argues, “[b]y distinguishing acceptable changes from not unacceptable changes, mSIGNIA has limited its claims to particular predicted changes that are acceptable, and has disclaimed allowing every change that is not unacceptable.” (Dkt. 37 at 18.)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

The plain claim language itself refers to relying on “information regarding anticipated changes” to determine whether a particular change in a data value is “acceptable.” mSIGNIA doesn’t dispute this. Nor does mSIGNIA dispute that this claim language, on its face, doesn’t relate to evaluating whether a data value is unacceptable by simply comparing it to a threshold value. Again, it appears that mSIGNIA’s statements were not related to disclaiming some aspect of the full plain and ordinary meaning of the claim language, but rather to distinguishing a prior art system that is simply different from the plainly understood claim language. Moreover, so long as an accused system evaluates anticipated changes to determine whether a change is acceptable, it could meet this claim limitation even if the system *also* evaluated whether a data value is unacceptable because it exceeded a defined threshold. Indeed, this is consistent with mSIGNIA’s statements in the POPR, which simply distinguished the prior art by observing that “*merely* reject[ing] unacceptable changes, just like a username/password system or any other prior art authentication system,” (*see* Dkt. 36-2 at 3 (emphasis added)) does not meet the claim limitation. InAuth’s proposed construction, then, might cause confusion if a fact-finder didn’t understand this distinction. These concerns outweigh InAuth’s arguments regarding the potential for mSIGNIA mischief.

No construction is necessary for the terms (1) “wherein such determining comprises using the stored information regarding anticipated changes to the stored data values associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value”; (2) “wherein such determining comprises using the stored information regarding anticipated changes to the stored data values to determine whether a data value used to form the identity claim is based on an acceptable change to a corresponding stored data value associated with the identity”; and (3) “wherein such determining comprises using the stored information regarding anticipated changes to the stored data values to determine whether a data value upon which the communication is based reflects an acceptable change to a corresponding stored data value associated with the identity.”

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

3.2.3. “user minutia data values” (Claims 3, 4, 5, and 6) and “user customization” (Claims 5, 11)

Although mSIGNIA briefed the terms “user minutia data values” and “user customization” separately in its opening brief, the parties end up discussing the terms together. The Court will do the same.

• **“user minutia data values” (Claims 3, 4, 5, and 6)**

mSIGNIA’s Proposed Construction	InAuth’s Proposed Construction
“data values reflecting changes and customizations made as a result of device usage (i.e., by the user)”	Plain and ordinary meaning

• **“user customization” (Claims 5, 11)**

mSIGNIA’s Proposed Construction	InAuth’s Proposed Construction
“software data value changes introduced to the computer by the user”	Plain and ordinary meaning

The parties’ dispute regarding the terms “user minutia data values” and “user customization” essentially boils down to whether these terms can relate to changes to computer hardware. mSIGNIA argues that both terms should be understood to only relate to changes a user makes to a device’s software. Stated differently, mSIGNIA argues that a data value or customization only relates to a “user” when it relates to someone using a device. If someone is changing a device by updating the hardware or firmware, mSIGNIA argues that the person are no longer acting as a “user” and those actions should not be considered in the construction of “user minutia data values” or “user customization.” InAuth argues that the plain meaning of the terms is broader, encompassing any changes made by a user to a computer’s hardware, firmware, or software.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

The term “user minutia data values” appears in dependent Claims 3, 4, 5, and 6. The term “user customization” appears in Claims 5 and 11. The claims themselves include some specific examples of what constitutes “user minutia data values” (including “user customization” as one type of user minutia data value). Claims 3 through 6 recite:

3. The identity recognition system of claim 1, wherein the challenge prompts a response based on one or more ***user minutia data values***.

4. The identity recognition system of claim 3, wherein the operation of determining whether the response is allowable includes evaluating whether at least a portion of the response is based on one or more acceptable changes to a ***user minutia data value***.

5. The identity recognition system of claim 4, wherein the ***user minutia data values*** used to determine whether the response is allowable comprise user secrets, ***user customization***, entertainment data, bio-metric data, or contacts.

6. The identity recognition system of claim 4, wherein the ***user minutia data values*** used to determine whether the response is allowable comprise calling app data, geo-location data, frequently called phone numbers, email, or network connection data.

’852 Patent, Claims 3–6 (emphasis added). mSIGNIA observes (without relying on any support) that the term “user customization” as used in Claim 5 appears in a list of “software data values that are specific to or customized by the user.” (Dkt. 38 at 6.)

By contrast, some of the other dependent claims refer more generally to what would be considered acceptable data values from a computer. For instance, Claims 10 through 12 explain that acceptable values might be based on “industry updates to hardware, firmware, or software elements,” “an anticipated ***user customization*** of the computer,” or “anticipated usage of the computer by a user.” *See* ’852 Patent, Claims 10–12 (emphasis added). Notably, these claims use both the phrases “user customization” and “usage of the computer by a

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

user.” They also juxtapose “industry updates to hardware, firmware, or software elements” against “user customization of the computer” generally.

The specification refers to “computer and user minutia” by stating it is, “e.g., any piece of information that can be definitively associated with the computer and its user, including information from the general categories of what the user or computing device has, what the user knows, and what the user is.” ’852 Patent at 6:30–35. When later discussing a particular embodiment, the ’852 Patent also refers to concepts of hardware, firmware, and software minutia, explaining,

[h]ardware minutia values typically cannot change without changing a physical component of the computer **18**. Firmware minutia can be updated but usually their update is controlled by someone other than the service user **20**. Software minutia changes dynamically via various individual instantiations of service user **20** and includes elements that may require predictable, constant change in normal situations (i.e., frequently called contact phone numbers).

Id. at 11:38–46. This list, however, doesn’t specifically put “user minutia” into a particular bucket of hardware, firmware, or software minutia.

The specification explains the concept of “customizations performed by the service user **20**” in the sentences that immediately follow in the context of software minutiae, stating,

[i]t is important to note that software minutiae values can often reflect customizations performed by the service user **20**. In this manner, software minutiae values can accurately identify computer **18** devices that are otherwise extremely similar in hardware and firmware. When the computer **18** is manufactured, devices are very similar, hence the need for serial numbers, but, under security considerations, these hardware minutia identifiers are few in number and can be easily spoofed. Significant customization affecting software minutiae values is typically done within days, even hours, of ownership of a computer **18** by the service user **20**.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

Id. at 11:47–57. The ’852 Patent later provides some examples of user customization, again focusing on customization of software. The specification states that after receiving a new computer, a user will typically “customize the computer **18** with service user **20** specific information such as, for example, contacts, email and network connections. The customizations these additions represent (i.e. minutia) can immediately differentiate two examples of computer **18** that were manufactured one immediately after the other.” *Id.* at 13:26–31. But again, the specification doesn’t necessarily assert that “user customization” must necessarily be limited to changes to software.

Although mSIGNIA extrapolates from some of the language in the specification and one of the dependent claims, it doesn’t point to any instances in the specification where the inventors specifically excluded user changes to hardware from the meaning of these terms. On the current record, mSIGNIA hasn’t provided a sufficient basis to support limiting the meaning of these terms. That some of the specification’s examples describe user customization in the context of changes to software is insufficient.

mSIGNIA also relies on a “simple analogy” in its Responsive Claim Construction Brief to support its argument:

The user of an automobile is the one who uses it; while they are driving the vehicle, listening to the radio, or adjusting the air conditioner of the vehicle, they are the ‘user’ of that car. But if such person gets outside of the car and cleans the windshield, or changes the battery or the tires, they are *working on* the car, not *using* the car; they are no longer users. So, too, in the ’852 Patent, a user does not change the hardware or firmware on the claimed computer since during these actions they would no longer be the user of the computer. Instead, this type of maintenance, upgrade, or repair is done by a tinkerer, manufacturer, vendor, or repair shop.

(Dkt. 38 at 6.) But it’s too much of a stretch to say that an individual’s status as a “user” changes depending on the activities undertaken by the user. It’s still the user’s car – just like it’s still the user’s computer – to do with as the user pleases. Hanging an air freshener doesn’t

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES – GENERAL

Case No.	SACV 17-01289 AG (KESx)	Date	June 6, 2018
Title	MSIGNIA, INC. v. INAUTH, INC.		

transform a user into a tinkerer. Customizing the physical components of either a car or computer is simply another way a user might make it their own, for improved smell or performance or whatever other reason a user might have to make a customization.

mSIGNIA’s argument that the term “user” will be read out of the claims under InAuth’s construction is also unpersuasive. Indeed, InAuth’s “construction proposal” is that the terms be understood by their plain and ordinary meaning. Both terms include the term “user,” and InAuth does not appear to dispute that to be a “user minutia data value” or “user customization,” the user must be involved in either influencing the data value or making the customization. In comparison, for example, an *industry* update to hardware, firmware, or software will not necessarily be a user customization.

The term “minutia,” however, is not a term that every lay juror will readily know and understand. Although the Court concludes no construction is necessary for the term “user customization,” it construes the term “user minutia data values” as “data values that can be definitively associated with the user.”

4. DISPOSITION

These claim constructions shall govern in this case.

Initials of Preparer _____ : _____
